



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/896,380	06/29/2001	Gary L. Graunke	42390P11153	9543
7590	01/30/2006		EXAMINER	
Gordon R. Lindeen III			SHIFERAW, ELENI A	
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP			ART UNIT	PAPER NUMBER
12400 Wilshire Boulevard, Seventh Floor				2136
Los Angeles, CA 90025-1026				

DATE MAILED: 01/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/896,380	GRAUNKE, GARY L.	
	Examiner Eleni A. Shiferaw	Art Unit 2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 17 October 2005.
- 2a) This action is FINAL. 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-21 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-21 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|-------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____. | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| | 6) <input type="checkbox"/> Other: _____. |

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on October 17, 2005 has been entered.

2. Claims 1-21 are presented for examination.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 1-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kamiya et al. (Kamiya, Pub. No.: US 2002/0106086 A1) in view of Menezes et al. (Menezes, Handbook of Applied Cryptography).

As per claims 1 and 12, Kamiya discloses a method/medium/apparatus having stored thereon data representing sequences of instructions which, when executed by a machine, cause the machine to perform operations comprising:

receiving first and second encryption keys from a key server (claim 13 and 15, par. 0105 and 0118; *key generation unit providing keys...*);

receiving encrypted video from a broadcast video source (par. 0093, 0079, 0081, and 0098; *broadcasting encrypted video data to receivers...*);

generating a first cipher stream based on the first key for decrypting the encrypted video (par. Claim 15, par. 0043, 0171, 0169 lines 1-6, and par. 0030 lines 4-6; *encrypted first key to decrypt video data, and upstream system/content provider generates an encrypted digital data in using first key*);

generating a second cipher stream based on the second key (claim 15, par. 0043, 0017, 0174 and page 1 par. 0010; *generating encrypted key stream based on a second key*) to re-encrypt the decrypted video (par. 0123, 0127 and 0129; *the downstream system/receiver device re-encrypts the decrypted digital data for further protection*); and

conveying the re-encrypted video to a display device to be decrypted by the display device using the second key (par. 0129, [0136-0140] and fig. 4 No. 34).

Kamiya teaches simultaneously encrypting encryption keys and simultaneously decrypting encryption keys (0129). Kamiya fails to explicitly teach simultaneously decrypting and re-encrypting the encrypted video using a combination of the first and second cipher streams;

However Menezes discloses a cipher-chaining block (CBC) of multiple encryption method to simultaneously re-encrypting and decrypting plain text data using a combination of the first and the second cipher streams (page 233-237 section 7.2.3-7.42; simultaneously re-*encrypting data...E(x) = Ek2(Ek1(data))...decrypted simultaneously...*);

Therefore it would have been obvious to one having ordinary skill in the art at the time of the invention was made to employ the teachings of Menezes within the teachings of Kamiya

because it would allow to provide integrity and confidentiality of data (page 230 section 7.16).

One would have been motivated to modify the teachings of CBC (simultaneously encrypting and decrypting data) within the system of Kamiya because it would prevent data from being intercepted during decryption and re-encryption process when data is in clear.

As per claims 2 and 13, Kamiya and Menezes teach all the subject matter as described above. In addition Kamiya teaches the method/medium, wherein simultaneously decrypting and re-encrypting the encrypted video comprises exclusive OR-ing the encrypted video with the cipher stream combination (Kamiya page 9 par. 0123, 0127 and 0129; encrypted key and encrypted digital data are received separately and combined together to simultaneously decrypt the encrypted key and encrypted digital data and decrypted digital data is further encrypted by the receiver);

As per claims 3 and 14, Kamiya and Menezes teach all the subject matter as described above. In addition Kamiya teaches the method/medium, teach all the subject matter as described above. In addition Akiyama teach the method, wherein the cipher stream combination comprises a result of exclusive OR-ing the first and second cipher streams (Akiyama page 1 par. 0010-0012, and page 12 par. 0174; encrypted first key that is encrypted by second key and encrypted second key is combined and transmitted to the receiver).

As per claims 4 and 15, Kamiya and Menezes teach all the subject matter as described above. In addition Kamiya discloses the method/medium, wherein the first key and the second key have

symmetric agreement (Kamiya page 1 par. 21-24).

As per claims 5, 16 and 18, Kamiya and Menezes teach all the subject matter as described above. In addition Kamiya discloses the method/medium/apparatus, wherein receiving the first and second encryption keys comprises receiving one or more of the first key and the second key over a secure authenticated channel (Kamiya page par. 0023, page 4 par. 0047, and page 30 lines 4-6).

As per claim 6, Kamiya and Menezes teach all the subject matter as described above. In addition Kamiya discloses the method, wherein receiving a key over a secure authenticated channel comprises receiving the key from a sales server (Kamiya page 3 par. 0030 lines 4-6).

As per claim 7, Kamiya and Menezes teach all the subject matter as described above. In addition Kamiya discloses the method, wherein the secure authenticated channel comprises an Internet connection (Kamiya Page 8 par. 0014).

As per claim 8, Kamiya and Menezes teach all the subject matter as described above. In addition Kamiya discloses the method, wherein the secure authenticated channel comprises a telephone line (Kamiya Page 1 par. 0021, and page 3 par. 0045).

As per claims 9 and 20, Kamiya and Menezes teach all the subject matter as described above. In addition Kamiya discloses the method/apparatus, further comprising conveying the second key to the display device to enable the display device to decrypt the re-encrypted video (Kamiya page 9

par. 0123, 0127, 0129, & 0132, and fig. 4 No. 34).

As per claim 10, Kamiya and Menezes teach all the subject matter as described above. In addition Kamiya discloses the method, wherein the encrypted video is publicly available and encrypted with a public key and wherein the first key is a locally available private key (Kamiya page 2 par. 0021).

As per claim 11, Kamiya and Menezes teach all the subject matter as described above. In addition Kamiya discloses the method, wherein the encrypted video is a broadcasted entertainment program (Kamiya page 5 par. 0074 lines 5-10).

As per claim 19 Kamiya and Menezes teach all the subject matter as described above. In addition Kamiya teaches the apparatus, wherein the first key and the second key have symmetric agreement (Kamiya page 1 par. 21-24) and wherein the combination of the first and the second cipher streams is a result of exclusive OR-ing the encrypted video with an encryption stream (Akiyama page 1 par. 0010-0012, and page 12 par. 0174; encrypted first key that is encrypted by second key and encrypted second key is combined and transmitted to the receiver).

As per claim 20, Kamiya and Menezes teach all the subject matter as described above. In addition Kamiya discloses the apparatus, wherein the computing device conveys the second key to the display device to enable the display device to decrypt the re-encrypted video (Kamiya Page 2 par. [0031-0032]).

As per claim 21, Kamiya and Menezes teach all the subject matter as described above. In addition Kamiya discloses the apparatus, wherein the computing device includes a broadcast entertainment set-top box (Kamiya page 5 par. 0074 lines 5-10, and page 7 par. 0098 lines 1-3).

Conclusion

5. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

EP 0 926 894 A1: *Tranchard et al. discloses simultaneously encrypting and decrypting television video data to control access.*

US 4,642,688: *Lowry et al. teaches simultaneously decrypting and encrypting television signal for low cost, small storage and more reliable in operation.*

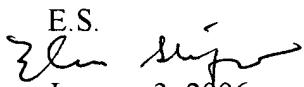
JP 11-2521177 A: *Ishii teaches a ciphering device simultaneously ciphering digital video data.*

US 6,154,542: *Crandall discloses simultaneously encrypting and/or decrypting for fast cryptography processing.*

6. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Eleni A. Shiferaw whose telephone number is 571-272-3867. The examiner can normally be reached on Mon-Fri 8:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

E.S.

January 3, 2006

CL
Primary Examiner
AVU31
1/5/06